State of Tennessee

Department of Health

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)
Policies and Procedures Manual

STATE OF TENNESSEE
DEPARTMENT OF HEALTH
CORDELL HULL BUILDING
425 5th AVENUE NORTH
NASHVILLE, TN 37247

MEMORANDUM

DATE: April 11, 2003

TO: All Bureaus, Offices and Programs

FROM: Kenneth S. Robinson, M.D., Commissioner

SUBJECT: Health Insurance Portability & Accountability Act (HIPAA) Policies and Procedures

The Tennessee Department of Health is obligated to implement the Health Insurance Portability and Accountability Act (HIPAA). A HIPAA Policies and Procedures Manual has been developed for your instruction in following the requirements of HIPAA.

All Department of Health's bureaus, offices, regional offices, local health departments, and program areas are directed to follow all applicable policies and procedures found in the HIPAA Policies and Procedure Manual.

The manual currently includes only policies pertaining to the privacy section of HIPAA. As policies are developed pertaining to standard transaction, codes sets, and identifiers and security, these sections will be forwarded to you for inclusion to the manual under sections two and three.

This manual shall be accessible at each Department of Health's location and in the Central Office. Failure to comply with this manual may result in disciplinary sanctions.

Thank you for your adherence to these policies and procedures.

State of Tennessee
Department of Health
Health Insurance Portability and Accountability Act (HIPAA)
Policies and Procedures Manual

Table of Contents

HIPAA Privacy Policies and Procedures
Section One

HIPAA Standard Transaction, Codes Sets, and Identifiers Policies and Procedures Section Two

---

HIPAA Security Policies and Procedures Section Three

Tennessee Department of Health

HIPAA Policies

Privacy

Policy Title: Administrative Requirements for the Implementation of HIPAA

Policy Number: 101

Effective Date: April 14, 2003

PURPOSE:

To issue instructions to all bureaus, offices, programs and workforce members regarding the Department of Health's (DOH) obligations relating to the implementation of the Health Insurance Portability and Accountability Act (HIPAA), 42 U.S.C. §§1320d-1329d-8, and regulations promulgated thereunder, 45 CFR Parts 160 and 164. This policy outlines DOH general guidelines and expectations for the necessary collection, use, and disclosure of protected health information (PHI) about clients in order to provide services and benefits to individuals while maintaining reasonable safeguards to protect the privacy of their information.

Definitions:

Protected Health Information (PHI) means individually identifiable information relating to past, present or future physical or mental health or condition of an individual, provision of health care to an individual, or the past, present or future payment for health care provided to an individual.

Workforce Members means employees, volunteers, trainees, contractors, and other persons whose conduct, in the performance of work for the department, its offices, or programs is under the direct control of the department, office, or program regardless of whether they are paid by the DOH.

Client for the purpose of HIPAA is defined as an individual for whom the DOH uses or maintains protected health information such as:

1. birth and death records,
2. infectious disease records,
3. health registries,
4. statistical data,
5. information obtained through an investigative or certification process of the DOH, etc., and
6. those who apply for or receive health services through DOH.

Licensee is a person or entity that applies for or receives 1) a license, 2) a certification, or 3) a registration, or similar authority from DOH to perform or conduct a service, activity or function.

Provider is a person or entity who may seek reimbursement or payments from DOH as a provider of services to DOH clients. (Not pertaining to DOH when DOH is a direct provider of services)

Treatment, Payment and Health Care Operations (TPO) includes all of the following:

- *Treatment* means the provision, coordination, or management of health care and related services, consultation between providers relating to an individual, or referral of an individual to another provider for health care.
- *Payment* means activities undertaken to obtain or provide reimbursement for health care, including determinations of eligibility or coverage, billing, collection activities, medical necessity determinations and utilization review.
- *Health Care Operations* include functions such as quality assessment and improvement activities, reviewing competence or qualifications of health care professionals, conducting or arranging for medical review, legal services, and auditing functions, business planning and development, and general business and administrative activities.

POLICY:

General Overview

DOH may collect, maintain, use, transmit, share and/or disclose information about clients, providers, and licensees, to the extent needed to administer DOH programs, services and activities. DOH will safeguard all PHI about clients, providers, and licensees, inform clients, providers, and licensees about DOH'S privacy practices and respect clients', providers', and licensees' privacy rights, to the full extent required under this policy.

This policy identifies two types of individuals of whom DOH is most likely to obtain, collect or maintain individual information:

i) DOH clients;

ii) Licensees or providers.

DOH, its workforce, and business associates will respect and protect the privacy of records and information about clients who request or receive services from DOH and licensees and providers. All information must be safeguarded in accordance with DOH privacy policies and procedures.

DOH has adopted reasonable policies and procedures for administration of its programs, services and activities. If any state or federal law or regulation, or order of a court having appropriate jurisdiction, imposes a stricter requirement upon any DOH policy regarding the privacy or safeguarding of information, DOH shall act in accordance with the stricter standard.

DOH staff shall act in accordance with established DOH policy and procedures regarding the safeguarding of client information, whether health-related or not, in all DOH programs, services and activities. In the event that more than one policy applies but compliance with all such policies cannot reasonably be achieved, the DOH employee will seek guidance from supervisors according to established DOH policy and procedures. DOH staff should consult with their Subsidiary Privacy Officer or the Department Privacy Officer in appropriate circumstances.

DOH Notice of Privacy Practices

A. The current "***DOH Notice of Privacy Practices***" shall be available in all offices of the DOH.

B. DOH will provide a copy of the current "***DOH Notice of Privacy Practices***" to any client who requests a copy. However, where DOH is a direct provider to the client, DOH is required to give a copy of the notice to the client on the first date that they receive services on or after April 14, 2003. DOH must have each client who receives direct care from DOH sign an acknowledgment of receiving the notice on their first date of service. If DOH cannot get a signed acknowledgement, then documentation as to the reason why one was not received must be made in the client's record. Acknowledgment of receipts of the notice, and/or documentation of good faith effort to obtain written acknowledgement must be maintained for six years.

C. The "***DOH Notice of Privacy Practices***" shall contain all information required under federal regulations regarding the notice of privacy practices for protected health information under HIPAA.

D. The "***DOH Notice of Privacy Practices***" shall also be available at the DOH website.

E. Whenever the notice is revised, it should be made available upon request and posted on or after the effective date of revision.

F. Copies of the notice and all revisions shall be maintained by the Department Privacy Officer.

Administrative Requirements

Due to HIPAA requirements, DOH has implemented certain administrative requirements as specified below:

A. Personnel Designations

1. Department Privacy Officer**:** The DOH must designate an individual to be the Department Privacy Officer, responsible for the development

and implementation of department-wide policies and procedures relating to the safeguarding of PHI.

2. Subsidiary Privacy Officers will be appointed to represent bureaus/ offices, regional office and local health departments, and to act in support of the Department Privacy Officer.

B. Privacy Officers Duties

1. The Department Privacy Officer will oversee all ongoing activities related to the development, implementation, and maintenance of, and adherence to the department's policies concerning privacy. Establish and administer a process for receiving, documenting, tracking, investigating, and taking action on all complaints. Ensure that the Department is 1) in compliance with its privacy practices, and 2) consistently applies sanctions for failure to comply with privacy policies for all individuals in the Department's workforce and business associates.

2. Subsidiary Privacy Officers will be responsible for providing information about DOH'S privacy practices and receiving complaints relating to PHI and forwarding these to the Department Privacy Officer.

C. Workforce Training Requirements

The DOH and, as applicable, its bureaus/offices must document the following training actions:

1. On or before April 14, 2003, all DOH workforce members must receive HIPAA awareness training. Training regarding appropriate policies and procedures relating to PHI will be given as necessary and appropriate for those employees whose jobs are impacted by HIPAA.

2. After April 14, 2003, each new workforce member, or a workforce member reporting to work for the first time since April 14, 2003, shall receive the training as described above within a reasonable time after joining or re-joining the workforce.

3. After training as described above has been given to all the current workforce, DOH shall require every workforce member to sign a

revised "Confidentiality Statement" (Form PH. 3131). All new workforce members shall sign the "Confidentiality Statement" as soon as they have received the appropriate training as outlined above.

4. Each workforce member must receive training as described above within a reasonable time when:

   a. a material change in the policies and procedures relating to PHI occurs and it impacts his/her work, or

   b. a change in jobs or position responsibilities occurs.

D. Policies and Procedures

NOTE: The HIPAA Privacy Policies become effective on April 14, 2003. However, a reasonable time will be given bureaus/offices to become completely compliant with these policies in their program areas. Each bureau/office shall strive to achieve compliance in all areas as soon as feasible.

The DOH and, as applicable, its bureaus/offices must document the following actions relating to its policies and procedures:

1. The DOH shall design and implement policies and procedures to assure appropriate safeguarding of PHI in its operations to be followed by all workforce members.

2. The DOH must change its policies and procedures as necessary and appropriate to conform to changes in law or regulation. The DOH may also make changes to policies and procedures at other times as long as the policies and procedures are still in compliance with applicable law. Where necessary, DOH must make correlative changes in its privacy notice. The DOH may not implement a change in policy or procedure prior to the effective date of the revised privacy notice when required.

3. The DOH, and each bureau/office must maintain the required policies and procedures in written or electronic form, and must maintain written or electronic copies of all communications, actions, activities or designations as are required to be documented hereunder, or otherwise under the HIPAA regulations, for a period of six (6) years from the later

of the date of creation or the last effective date or such longer period that may be required under state or other federal law.

4. Policies and procedures have been developed for the following administrative requirements:

   a. Safeguarding PHI from intentional or unintentional unauthorized use or disclosure as outlined in **DOH HIPAA Policy #105,** *"Administrative, Technical, and Physical Safeguards."*

   b. Complaint process for documenting and referring complaints received by clients as outlined in **DOH HIPAA Policy #102,** *"Clients' Privacy Rights."*

   c. Application of sanctions and documentation of the application of appropriate sanctions against workforce members as outlined in **DOH HIPAA Policy #109**, *"Enforcement, Sanctions, and Penalties for Violations of Individual Privacy."*

   d. Each bureau/office must mitigate, to the extent practicable, any inappropriate use or disclosure of PHI by DOH or any of its business associates as outlined in **DOH HIPAA Policy #110,** *"Mitigation Efforts."*

   e. Neither the DOH nor any bureau/office or workforce member shall intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise of his/her rights relating to HIPAA compliance nor will DOH require clients to waive their rights to file a complaint as a condition for providing treatment, payment, or receiving a service, as outlined in **DOH HIPAA Policy #102**, *"Clients' Privacy Rights."*

5. Policies and procedures for other aspects of HIPAA have been developed to address operational issues as follows:

   a. Clients' rights to access their own information, with some exceptions, as well as the client's right to request restrictions or amendments to their information is outlined in **DOH HIPAA Policy #102**, *"Clients' Privacy Rights."*

b. The requirements DOH needs to follow regarding the uses and disclosures of client information is outlined in **DOH HIPAA Policy #103,** *"Uses and Disclosures of Client Information."*

c. DOH will use or disclose only the minimum necessary information necessary to provide services and benefits to clients as outlined in **DOH HIPAA Policy #104**, *"Minimum Necessary Information."*

d. DOH may use or disclose client's information for research purposes as outlined in **DOH HIPAA Policy #106,** *"Use and Disclosure for Research Purposes and Waivers."*

e. DOH staff will follow standards under which client information can be used and disclosed if information that can identify a person has been removed or restricted to a limited data set as outlined in **DOH HIPAA Policy #107**, *"De-identification of client information and Use of Limited Data Sets."*

f. DOH may disclose protected health information to business associates with whom there is a written contract or memorandum of understanding as outlined in **DOH HIPAA Policy #108,** *"DOH Business Associates."*

Reference(s):
• 45 CFR Parts 160 and 164
Contact(s):
• Privacy Program Office, (615) 253-5417

Tennessee Department of Health

HIPAA Policies

Privacy

Policy Title: Clients' Privacy Rights

Policy Number: 102

Effective Date: April 14, 2003 **Revised: February 18, 2010**

PURPOSE:

The intent of this policy is to establish the privacy rights that DOH clients have regarding the use and disclosure of their protected health information (PHI) that is held by DOH, and to describe the process for filing a complaint should clients feel those rights have been violated.

POLICY:

General
DOH will use the **"DOH Notice of Privacy Practices"** to inform clients about how DOH may use and/or disclose their information. The **"DOH Notice of Privacy Practices"** also describes the actions a client may take, or request DOH to take, with regard to the use and/or disclosure of their information.

The policies related to the **"DOH Notice of Privacy Practices"** and the distribution of the notice is addressed in **DOH HIPAA Policy #101,** "Administrative Requirements for the Implementation of HIPAA."

A. DOH clients have the right to, and DOH may not deny, the following:

1. Access to their own information, consistent with certain limitations;

a. Clients have the right to access, inspect, and obtain a copy of information on their own cases in DOH files or records, consistent with federal and Tennessee law. DOH will recognize the right of the personal representative of a deceased client to obtain a copy of PHI for the deceased. However, death certificates with cause of death will only be released in accordance with T.C.A. §68-3-205.

b. All requests for access will be made in writing in accordance with the appropriate bureau/office policy and procedure.

c. If DOH maintains information about the client in a record that includes information about other people, the client is only authorized to see information about him or her, except as provided below:

   i) If a person identified in the file is a minor child of the client, and the client is authorized under Tennessee law to have access to the minor's information or to act on behalf of the minor for making decisions about the minor's care, the client may also obtain information about the minor.

   ii) If the person requesting information is recognized under Tennessee law as a legal guardian or legal custodian of the client and is authorized by Tennessee law to have access to the client's information or to act on behalf of the client for making decisions about the client's services or care, DOH will release information to the requestor.

d. DOH must act on a client's request for access no later than 30 days after receiving the request, except:

   i) In cases where the information is not maintained or accessible to DOH on-site, DOH must act on the client's request no later than 60 days after receiving the request.

   ii) If DOH is unable to act within these 30-day or 60-day limits, DOH may extend this limitation by up to an additional 30 days, subject to the following:

      - DOH must notify the client in writing of the reasons for the delay and the date by which DOH will act on request.

- DOH will use only one such 30-day extension to act on a request for access.

e. If DOH grants the client's request, in whole or in part, DOH must inform the client of the access decision and provide the requested access.

i) If DOH maintains the same information in more than one format (such as electronically and in a hard-copy file) or at more than one location, DOH need only provide the requested protected information once.

ii) DOH must provide the requested information in a form or format requested by the client, if readily producible in that form or format. If not readily producible, DOH will provide the information in a readable hard-copy format or such other format as agreed to by DOH and the client.

iii) DOH may provide the client with a summary of the requested information, in lieu of providing access, or may provide an explanation of the information if access had been provided, if:

- The client agrees in advance; and
- The client agrees in advance to any fees.

iv) DOH must arrange with the client for providing the requested access in a time and place convenient for the client and DOH. This may include mailing the information to the client if the client so requests or agrees.

v) Fees: DOH may impose a fee for these records, in accordance with departmental regulations and/or policies.

vi) If DOH does not maintain the requested protected information, and knows where such information is maintained (such as by a medical provider, insurer, other public agency, private business, or other non-DOH entity), DOH must inform the client of where to direct the request access.

2. The DOH can deny access to the client to his PHI under the following limitations:

a. DOH may deny clients access to his own health information if federal law prohibits the disclosure. Under federal law, clients have the right to access, inspect, and obtain a copy of their own health information in DOH files or records **except for**:

i) Information that, in good faith, DOH believes can cause harm to the client, or to any other person;

ii) Information that was obtained from someone other than a health care provider under a promise of confidentiality, and access would reveal the source of the information;

iii) Information compiled for use in civil, criminal, or administrative proceedings;

iv) Information that is subject to the federal Clinical Laboratory Improvement Amendments of 1988, or exempt pursuant to 42 CFR 493.3(a)(2);

v) Documents protected by attorney work-product privilege; and

vi) Information where release is prohibited by state or federal laws.

b. Before DOH denies a client or their personal representative access to their information because there is a good faith belief that its disclosure could cause harm to the client or to another person, the DOH's decision to deny must be made by a licensed health care professional or other designated staff. DOH must make a review of this denial available to the client. If the client wishes to have this denial reviewed, the review must be done by a licensed health care professional who is part of the DOH workforce and who was not involved in the original denial decision.

DOH must promptly refer a request for review to the designated reviewer within the time frame of this policy.

The reviewer must determine, within a reasonable time, whether or not to approve or deny the client's request for access, in accordance with this policy.

The Departmental Privacy Officer must then:

i) Promptly notify the client in writing of the reviewer's determination; and

ii) Take action to carry out the reviewer's determination.

If DOH denies access, in whole or in part, to the requested information, DOH must:

i) Give the client access to any other requested client information, after excluding the information to which access is denied;

ii) Provide the client with a timely written denial.

The denial must:

i) Be sent or provided within the time limits specified in this policy;

ii) State the basis for the denial, in plain language;

iii) If the reason for the denial is due to danger to the client or another, explain the client's review rights as specified in this policy, including an explanation of how the client may exercise these rights; and

iv) Provide a description of how the client may file a complaint with DOH, and if the information denied is protected health information, with the United States Department of Health and Human Services, Office for Civil Rights, pursuant to this policy.

B. Rights of clients to an accounting of disclosures of protected health information

1. Clients have the right to receive an accounting of disclosures of protected health information (PHI) that DOH has made for any period of time, not to

exceed six years, preceding the date of requesting the accounting. This right does not apply to disclosures made prior to April 14, 2003; however, a bureau/office may disclose prior to that date.

2. The accounting is only required to include health information NOT previously authorized by the client for use or disclosure, and not collected, used or disclosed for treatment, payment or health care operations for that client or for purposes described in **"DOH Notice of Privacy Practices."**

3. Clients may make request for an accounting of disclosure at any DOH office, either in the central office, or at a regional or local office. The office where the request is received is required to only make an accounting of the disclosures that were made by that office. When the accounting is made to the client, each office should include a statement that indicates that this is an accounting of disclosures for their particular office only, i.e. "This is an accounting of the disclosures made by the Wilson County Health Department only. If you are interested in whether or not other disclosures may have been by the DOH, please contact the Tennessee Department of Health Privacy Officer at ....."

4. The Department Privacy Officer will be responsible for the accounting of disclosures received by his office. The Department Privacy Officer will do all the research to assure the accounting includes disclosure for the entire department and will issue the accounting to the client.
5. All requests for an accounting of disclosures will be made in writing by client.

6. Disclosures that are not required to be tracked and accounted for by DOH are those that are:
   a. Made within DOH;

   b. Authorized by the client;

   c. Made prior to April 14, 2003;

   d. Made to carry out treatment, payment, and health care operations;

e. Made to the client;

f. Made as part of a limited data set in accordance with the **DOH HIPAA Policy #107,** "De-identification of Client Information and Use of Limited Data Sets";

h. For national security or intelligence purposes;

i. Required by law;

j. Made to a business associate and/or other state agencies covered by a Memorandum of Understanding; or

k. Covered under a disclosure protocol for that appropriate office.

7. Disclosures that are required to be tracked must be done in accordance with the appropriate bureau/office policy and procedure. The accounting must include, for each disclosure:

a. The date of the disclosure;

b. The name, and address, if known, of the person or entity who received the disclosed information;

c. A brief description of the information disclosed; and

d. A brief statement of the purpose of the disclosure that reasonably informs the client of the basis for the disclosure, or, in lieu of such statement, a copy of the client's written request for a disclosure, if any.

8. DOH will temporarily suspend a client's right to receive an accounting of disclosures that DOH has made to a health oversight agency or to a law enforcement official, for a length of time specified by such agency or official, if:

   a. The agency or official provides a written statement to DOH that such an accounting would be reasonably likely to impede their activities.

   b. However, if such agency or official makes an oral request, DOH will:

      i) Document the oral request, including the identity of the agency or official making the request;

      ii) Temporarily suspend the client's right to an accounting of disclosures pursuant to the request; and

      iii) Limit the temporary suspension to no longer than 30 days from the date of the oral request, unless the agency or official submits a written request specifying a longer time period.

9. DOH must act on the client's request for an accounting no later than 60 days after receiving the request, subject to the following:

   1. If unable to provide the accounting within 60 days after receiving the request, DOH may extend this requirement by another 30 days. DOH must provide the client with a written statement of the reasons for the delay within the original 60-day limit, and inform the client of the date by which DOH will provide the accounting.

   2. DOH will use only one such 30-day extension.

   3. In addition to the accounting of disclosures that is given to a client, a copy of any disclosure protocol should also be given to the client which indicates that if any of the situations described in the protocol were met, his PHI may have been disclosed to the specified agency.

C. Rights of clients to file complaints regarding disclosure of information

1. Clients have a right to submit a complaint if they believe that DOH has improperly used or disclosed their protected information, or if they have concerns about the privacy policies of DOH or concerns about DOH compliance with such policies.

2. Complaints may be filed with any of the following:

   a. The Tennessee Department of Health's HIPAA Privacy Officer

   b. The U.S. Department of Health and Human Services, Office for Civil Rights.

   c. The Subsidiary Privacy Officers may receive complaints and then forward them to the Department Privacy Officer.

3. The DOH workforce will not intimidate, threaten, coerce, discriminate against, or take any other form of retaliatory action against any person filing a complaint or inquiring about how to file a complaint.

4. The DOH workforce may not require clients to waive their rights to file a complaint as a condition of providing of treatment, payment, enrollment in a health plan, or eligibility for benefits.

5. The Department Privacy Officer will review and determine action on complaints filed with DOH. The Department Privacy Officer will also perform these functions when DOH is contacted about complaints filed with the U.S. Department of Health and Human Services – Office for Civil Rights.

6. The Department Privacy Officer or his designee will receive, review and determine the action to be taken on all complaints. The Department Officer will document and maintain all complaints, the findings from reviewing each complaint, and DOH actions resulting from the complaint. For each specific complaint, this documentation shall include a description of corrective actions that DOH has taken, if any are necessary, or why corrective actions are not needed.

D. Clients may make specific requests regarding the use and disclosure of their information and DOH may either approve or deny the request. Specifically, clients have the right to request:

1. Restricted use and disclosure of their information

a. Clients have the right to request in writing restrictions on the use and/or disclosure of their information for:

i) Carrying out treatment, payment, or health care operations;

ii) Disclosure of health information to a relative or other person who is involved in the client's care;

b. DOH is not obligated to agree to a restriction and may deny the request or may agree to a restriction more limited than what the client requested; however, **DOH MUST comply with requests to restrict disclosure of PHI to a health plan for payment or health care operations IF the PHI pertains to health care items or services which were paid in full out of pocket by the patient or his/her representatives.**

Exception: Certain programs can only use information that is authorized by the client, such as alcohol and drug programs. (42 CFR Part 2) For those program clients, DOH shall honor their requests for restriction by making sure that the authorization clearly identifies the authorized recipients of the information.

c. DOH is not required to agree to a restriction requested by the client.

i) DOH will not agree to restrict uses or disclosures of information if the restriction would adversely affect the quality of the client's care or services.

ii) In an emergency situation, DOH may use or disclose such information to the extent needed to provide the emergency treatment to the client.

d. DOH will document the reasons for granting or denying the request for restriction in the client's hard copy or electronic record.

i) Prior to any use or disclosure of client information, DOH staff must confirm that such use or disclosure has not been granted a restriction by reviewing the client's case file.

e. DOH may terminate its agreement to a restriction if:

i) The client agrees to or requests termination of the restriction in writing;

ii) The client orally agrees to, or requests termination of the restriction. DOH will document the oral agreement or request in the client's DOH case record file; or

iii) DOH informs the client in writing that DOH is terminating its agreement to the restriction. Information created or received while the restriction was in effect shall remain subject to the restriction.

2. Rights of clients to request to receive information from DOH by alternate means or at alternate locations

a. DOH must accommodate reasonable requests by clients to receive communications by alternate means, such as by mail, e-mail, fax or telephone; and

b. DOH must accommodate reasonable requests by clients to receive communications at an alternate location.

c. In some cases, sensitive health information or health services must be handled with strict confidentiality under state law. For example, information about substance abuse treatment and certain sexually transmitted diseases may be subject to specific handling. DOH will comply with the more restrictive requirements.

3. Rights of clients to request amendments to their information.

a. Clients have the right to request that DOH amend their information in DOH files.

b. All requests for amendments must be made in writing and a justification must be given to support the request for the amendment in accordance with the appropriate bureau/office policy and procedure.

c. DOH is not obligated to agree to an amendment and may deny the requests or limit its agreement to amend. Prior to any decision, based on a client's request for DOH to amend a previously documented health or medical record, the bureau's medical director or a licensed health care professional designated by the bureau director shall review the request and any related documentation. The licensed health care professional may be a DOH staff person involved in the client's case.

d. Prior to any decision to amend any other information that is not a health or medical record, a DOH staff person designated by the program administrator shall review the request and any related documentation.

e. If DOH grants the request, in whole or in part, DOH must:

i) Make the appropriate amendment to the protected information or records, and document the amendment in the client's file or record;

ii) Provide timely notice to the client that the amendment has been accepted, pursuant to the time limitations of this policy;

iii) Seek the client's agreement to notify other relevant persons or entities with whom DOH has shared or needs to share the amended information of the amendment; and

iv) Make reasonable efforts to inform, and to provide the amendment within a reasonable time to:

- Persons named by the client as having received protected information and who thus need the amendment; and

- Persons, including business associates of DOH, which DOH know have the protected information that is the subject of the

amendment and that may have relied, or could rely, on the information to the client's detriment.

f. DOH may deny the client's request for amendment if:

i) DOH finds the original information to be accurate and complete;

ii) The information was not created by DOH, unless the client provides a reasonable basis to believe that the originator of such information is no longer available to act on the requested amendment;

iii) The information is not part of DOH records; or

iv) If it would not be available for inspection or access by the client, pursuant to this policy.

g. If DOH denies the requested alteration, in whole or in part, DOH must:

i) Provide the client with a timely written denial. The denial must:

- Be sent or provided within the time limits specified in this policy;
- State the basis for the denial, in plain language;
- Explain that if the client does not submit a written statement of disagreement, the client may ask that if DOH makes any future disclosures of the relevant information, DOH will also include a copy of the client's original request for amendment and a copy of the DOH written denial; and
- Explain the client's right to submit a written statement disagreeing with the denial and how to file such a statement. If the client does so:
  - DOH will enter the written statement into the client's DOH case file;
  - DOH may also enter a DOH written rebuttal of the client's written statement into the client's DOH case file. DOH will

send or provide a copy of any such written rebuttal to the client;

- DOH will include a copy of that statement, and of the written rebuttal by DOH if any, with any future disclosures of the relevant information; and

- Provide information on how the client may file a complaint with DOH, or with the U.S. Department of Health and Human Services, Office for Civil Rights.

h. DOH must act on the client's request no later than 60 days of receiving the request. If DOH is unable to act on the request within 60 days, DOH may extend this time limit by up to an additional 30 days, subject to the following:

• DOH must notify the client in writing of the reasons for the delay and the date by which DOH will act on the receipt; and

• DOH will use only one such 30-day extension.

E. Decisions related to any other requests made to DOH under this policy shall be handled in a manner consistent with federal and state statutes, rules and regulations and/or DOH policies and procedures applicable to the program, service or activity and shall be coordinated with DOH'S Privacy Officer.

Reference(s):
• 45 CFR Part 164.522 – 164.528
Contact(s):
• Privacy Program Office, (615) 741-1969

Tennessee Department of Health

HIPAA Policies

Privacy

Policy Title: Uses and Disclosures of Client Information

Policy Number: 103

Effective Date: April 14, 2003 **Revised February 18, 2010**

The intent of this policy is to specify when a client's protected health information (PHI) can be used or disclosed without the client's prior authorization. It will also specify how to use or disclose PHI when there is a client's authorization.

POLICY:

General – Client Authorization

DOH may disclose information for purposes of payment, treatment, and health care operations without client authorization unless otherwise required by bureau/office policy.

DOH shall not use or disclose any protected health information about a client of DOH programs or services without a signed authorization for release of that information from the client, or the client's personal representative, unless authorized by this policy, or as otherwise required by state or federal law.

A. A signed authorization is required in the following situations:

1. Prior to a client's enrollment in a DOH health service, if necessary for determining eligibility or enrollment;

2. For disclosures to an employer for use in employment-related determinations; and

3. For research purposes unrelated to the client's treatment;

2. For any purpose in which state or federal law requires a signed authorization.

B. DOH may obtain, use, or disclose information only if the written authorization (excluding authorization for TPO if required by bureau/office policy) includes all the required elements of a valid authorization. The required elements are:

1. A description of the information to be used or disclosed that identifies the purpose of the information in a specific and meaningful fashion;

2. The name or other specific information about the person(s), classification of persons, or entity (i.e., DOH or specified DOH program) authorized to make the specific use or disclosure;

3. The name or other specific identification of the person(s), classification of persons, or entity to whom DOH may make the requested use or disclosure;

4. An expiration date, or an expiration event that relates to the client or to the purpose of the use or disclosure;

5. Signature of the client, or of the client's personal representative, and the date of signature; and

6. If the client's personal representative signs the authorization form instead of the client, a description or explanation of the representative's authority to act for the client, including a copy of the legal court document (if any) appointing the personal representative, must also be provided.

C. Uses and disclosures must be consistent with what the client has authorized on the signed authorization form.

D. DOH may not require the client to sign an authorization as a condition of providing treatment services or to obtain payment for health care services.

E. Each authorization for use or disclosure of a client's information must be fully completed jointly by the staff member and the client, whenever possible, with the staff worker taking reasonable steps to ensure that the client understands why the information is to be used or released.

F. DOH must document and retain each signed authorization form for a minimum of six years.

G. When DOH receives a signed authorization from an outside entity, DOH must verify that it is a valid authorization (excluding authorization for TPO if required by bureau/office policy) and contains all the required information before DOH will release or disclose any PHI.

Use and Disclosures without a Client's Authorization

A. Public Health Authority/Activity

For the purpose of carrying out duties in its role as a public health authority, DOH does not need to obtain a client's authorization to lawfully receive, use, disclose or exchange PHI. Public health activity is defined as those duties necessary to prevent or control disease or injury; reporting vital events, such as births or deaths; and conducting public health surveillance, investigations, or interventions, etc.

1. Information about clients received or held by DOH as a governmental public health authority shall be safeguarded against loss, interception or misuse.

2. Allowable uses and disclosures for public health activities are as follows:

   a. A governmental public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability. This includes but is not limited to reporting disease, injury, vital events such as birth or death, and conducting public health surveillance, investigations, survey and certification, inspections, and interventions. Some of these types of disclosures may be covered in a disclosure protocol developed by each bureau/office and are included in the Department's accounting protocol;

b. An official of a foreign government agency that is acting in collaboration with a lawful governmental public health authority;

c. A governmental public health authority, or other appropriate government authority, that is authorized by law to receive reports of child abuse or neglect;

d. A person subject to the jurisdiction of the federal Food and Drug Administration (FDA), regarding an FDA-regulated product or activity for which that person is responsible, for activities related to the quality, safety, or effectiveness of such FDA-related product or activity. Such purposes include:

i) To collect or report adverse events, product defects or problems (including product labeling problems), or biological product deviations;

ii) To track FDA-related products;

iii) To enable product recalls, repairs, replacement, or look back; or

iv) To conduct post market surveillance.

3. A person who may have been exposed to a communicable disease or may be at risk of contracting or spreading a disease or condition. If DOH or other public health authority is authorized by law to notify such person as necessary in conducting a public health intervention or investigation.

a. As a public health authority, DOH is authorized to use and disclose a client's protected information in all cases in which DOH is permitted to disclose such information for the public health activities listed above.

b. Public health research will be conducted consistent with the **DOH HIPAA Policy #106,** *"Use and Disclosure for Research Purposes & Waivers."*

c. Where state or federal law prohibits or restricts uses and disclosure of information obtained or maintained for public health purposes, such use and disclosure shall be denied or restricted.

4. Operation of the Public Health Laboratory

   a. State law establishes that for the "protection of the public health," a public health laboratory is created within DOH to conduct tests and examinations at the request of any state, county, or city institution or officer, and at the request of any licensed physician.

   b. Laboratories are health care providers with an "indirect treatment relationship" as defined in federal regulations 45 CFR 164.501 and in accordance with 45 CFR 164.506 (a)(2)(i).

   c. DOH is authorized to use and disclose information for purposes of the operation of the public health laboratory consistent with HIPAA and applicable law.

5. Verifying the authority of a public health officer

   Health care providers and health care payers may request DOH to verify the authority of a DOH employee or contractor to conduct a public health activity. DOH employees or contractors must be prepared to explain and provide documentation to the provider or payer about their legal authority to collect or obtain information and be prepared to identify themselves.

B. Other Disclosures without Authorizations

To the extent not otherwise prohibited or limited by federal or state requirements applicable to the DOH program or activity, DOH may use or disclose protected information without the written authorization of the client in the following circumstances:

1. DOH may use or disclose PHI without a client's authorization if the law requires such use or disclosure, and the use or disclosure complies with, and is limited to, the relevant requirements of such law.

2. Internal communication within DOH is permitted without client authorization, in compliance with **DOH HIPAA Policy #104,** *"Minimum Necessary Information."* However, disclosure of alcohol and drug records may be limited to particular program areas named on their authorization form. If such a limitation is noted on the authorization form, disclosure is limited to the parties named.

3. DOH clients may access their own PHI with certain limitations in compliance with **DOH HIPAA Policy #102,** *"Clients' Privacy Rights."*

4. DOH may disclose information for purposes of payment, treatment, and health care operations without client authorization unless otherwise required by bureau/office policy.

5. If DOH has reasonable cause to believe that a child is a victim of abuse or neglect, DOH may disclose PHI to appropriate governmental authorities authorized by law to receive reports of child abuse or neglect.

   a. Consistent with applicable law, DOH may make reports and records available to any person, administrative hearing officer, court, agency, organization or other entity when the Department determines that such disclosure is necessary to:

      i) Administer the State's child welfare services and is in the best interests of the affected child;

      ii) Investigate, prevent or treat child abuse and neglect;

      iii) Protect children from abuse and neglect; or

      iv) Conduct research when the bureau director gives prior written approval.

   b. DOH may not disclose the names, addresses or other identifying information about the person who made the report.

6. If DOH has reasonable cause to believe that an adult is a victim of abuse or neglect, DOH may disclose PHI, as required by law, to a government authority authorized by law to receive such reports.

   a. If the disclosure is required by law and the disclosure complies with and is limited to the relevant requirements of such law; or

   b. If the client agrees to the disclosure, either orally or in writing; or

   c. When DOH staff, in the exercise of professional judgment and in consultation with an appropriate DOH supervisor, believes the disclosure is necessary to prevent serious harm to the client or other potential victims; or

   d. When the client is unable to agree because of incapacity, a law enforcement agency or other public official authorized to receive the report represents that:

      i) The protected information being sought is not intended to be used against the client, and

      ii) An immediate law enforcement activity would be materially and adversely affected by waiting until the client is able to agree to the disclosure.

   e. When DOH staff make a disclosure permitted above, DOH must promptly inform the client that such a report has been or will be made, except if:

      i) DOH staff, in the exercise of professional judgment and in consultation with an appropriate DOH supervisor, believes informing the client would place the client or another client at risk of serious harm; or

      ii) DOH staff would be informing a personal representative and DOH staff reasonably believes the personal representative is responsible for the abuse, neglect or other injury, and that informing such person would not be in the best interests of the client, as determined by DOH staff, in the exercise of

professional judgment and in consultation with the appropriate DOH supervisor.

7. DOH may use or disclose PHI without authorization for the purpose of carrying out its duties in its role as a health oversight agency. Such activities may be authorized by law, and include audits of health care providers; civil, criminal, or administrative investigations; prosecutions or actions; licensing or disciplinary actions; Medicare/TennCare fraud; or other activities necessary for oversight.

8. DOH may disclose information to a health oversight agency to the extent the disclosure is not prohibited by state or federal law for its oversight activities of:

   a. The health care system;

   b. Government benefit programs for which the information is relevant to eligibility;

   c. Entities subject to government regulatory programs for which the information is necessary for determining compliance with program standards; or

   d. Entities subject to civil rights laws for which the information is necessary for determining compliance.

9. Unless prohibited or otherwise limited by federal or state law applicable to the program or activity requirements, DOH may disclose client information without authorization for judicial or administrative proceedings in which the DOH or State is a party, in response to an order of a court, a subpoena.

10. As specified in HIPAA regulations 45 CFR 165.512, for limited law enforcement purposes to the extent authorized by applicable federal or state law, DOH may release PHI in the following circumstances: DOH may report certain injuries or wounds; provide information to identify or locate a suspect, victim, or witness; alert law enforcement of a death if suspected it is as a result of criminal conduct; and provide information which in good faith constitutes evidence of criminal conduct on DOH premises.

11. DOH may disclose PHI without authorization for research purposes, as specified in **DOH HIPAA Policy #106** *"Use and Disclosure for Research Purposes & Waivers."*

12. To avert a serious threat to health or safety, DOH may disclose client information without authorization if DOH believes in good faith that the information is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public; ***and*** the report is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat.

13. DOH may disclose client information without authorization for other specialized government functions, including authorized federal officials conducting lawful intelligence, counterintelligence, and other national security activities that federal law authorizes.

14. DOH may disclose limited information without authorization to a correctional institution or a law enforcement official having lawful custody of an inmate, for the purpose of providing health care or ensuring the health and safety of clients or other inmates.

15. In case of an emergency, DOH may disclose client information without authorization to the extent needed to provide emergency treatment.

16. The Family Educational Rights and Privacy Act (FERPA) and state law applicable to student records governs DOH access to, use, and disclosure of student records.

17. DOH may disclose information without authorization to another entity covered by federal HIPAA law and rules for the health care activities of that entity, if:

    a. Both that entity and DOH has or has had a relationship with the client who is the subject of the information;

    b. The information pertains to such relationship; and

c. The disclosure is for the purpose of:

i) Conducting quality assessment and improvement activities, including: outcome evaluation and development of clinical guidelines, provided that obtaining generalized knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs; protocol development; case management and care coordination; contacting health care providers and patients with information about treatment alternatives; and related functions that do not include treatment; or

ii) Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance; conducting training programs in which students, trainees or practitioners in areas of health care learn under supervision to practice or improvement their skills as health care providers; training of non-health care professionals; accreditation, certification, licensing, or credentialing activities; or

iii) Detecting health care fraud and abuse or for compliance purposes.

- Use or disclosures by DOH in training programs where students, trainees, learn under supervision to practice or improve their skills;

- To the extent authorized under state law to defend DOH in a legal action or other proceeding brought by the client.

18. If a health oversight activity or investigation is conducted in conjunction with an oversight activity or investigation relating to a claim for public benefits not related to health, the joint activity is considered a health oversight activity for purposes of this section.

19. When DOH is acting as a health oversight agency, DOH may use information for health oversight activities as permitted under this section.

20. DOH may use or disclose information without the written authorization of the client when DOH discloses information in a judicial or administrative proceeding subject to the following:

    a. DOH must follow any DOH procedures for responding to subpoenas, discovery requests, or other requests for documents that DOH may have regarding a client; DOH must not ignore any subpoena or other legal document.

        i) An administrative hearing officer or administrative law judge lacks legal authority, under Tennessee law, to require or authorize DOH to disclose information about a client that is confidential under federal or state law without appropriate subpoenas, orders, or similar lawful process. DOH staff should work with hearing officers to ensure that protective orders are used when appropriate in contested case hearings to prevent authorized uses and disclosures of information.

        ii) DOH staff will refer any questions or concerns regarding what is required by law, or by a court order, to the DOH Privacy Officer, who will then consult with the Office of General Counsel to resolve the question.

21. If DOH is sued or if a suit is filed on behalf of DOH, the Office of General Counsel will address or respond to legal issues related to the use and disclosure of information. DOH will identify confidentiality issues for discussion with the assigned legal counsel, in consultation with the DOH Privacy Officer, when deemed appropriate.

22. If DOH has obtained information in performing its duties as a health oversight agency, public health authority, nothing in this section supersedes DOH policies that otherwise permit or restrict uses or disclosures. For example, if DOH has obtained client patient information as a result of an oversight action against a provider, DOH may lawfully use that patient information in a hearing consistent with the other confidentiality requirements applicable to that program, service or activity.

23. In any situation in which federal or state law prohibits or restricts the use or disclosure of information in an administrative or judicial

proceeding, DOH shall assert the confidentiality of such confidential information, consistent with DOH policies applicable to the program, service or activity, to the presiding officer at the proceeding. A HIPAA-authorized protective order may not be sufficient to authorize disclosure if it does not address other applicable confidentiality laws.

24. DOH may disclose information in compliance with, and limited to the relevant specific requirements of:

    a. A court order or warrant, summons or subpoena issued by a judicial officer;

    b. A grand jury subpoena; or

    c. An administrative request, including administrative subpoena or summons, a civil or authorized investigative demand, or similar lawful process, provided that the information is relevant, material, and limited to a legitimate law enforcement inquiry.

    - **Exception:** Information on alcohol or drug treatment services can be disclosed only on the basis of a court order (42CFR Part 2)

25. DOH may disclose information to authorized federal officials for conducting lawful intelligence, counterintelligence, and other national security activities, as authorized by the federal National Security Act (50 U.S.C 401, et seq.) and implementing authority.

26. DOH may disclose information to authorized federal officials for the protection of the President or of other persons authorized by applicable federal law.

Client's authorization that is <u>not required</u> if they are informed in advance and given a chance to object

In some limited circumstances, DOH may use or disclose an client's information without authorization, but only if the client has been informed in advance and has been given the opportunity to either agree or to refuse or restrict the use or disclosure. These circumstances are:

For disclosure of health care information to a family member, other relative, or close personal friend of the client, or any other person named by the client, subject to the following limitations:

A. DOH may reveal only the protected information that directly relates to such person's involvement with the client's care or payment for such care.

B. DOH may use or disclose protected information for notifying (including identifying or locating) a family member, personal representative, or other person responsible for care of the client, regarding the client's location, general condition, or death.

C. If the client is present for, or available prior to, such a use or disclosure, DOH may disclose the protected information if it:

   1. Obtains the client's agreement;

   2. Provides the client an opportunity to object to the disclosure, and the client does not express an objection; or

   3. Reasonably infers from the circumstances that the client does not object to the disclosure.

D. If the client is not present, or the opportunity to object to the use or disclosure cannot practicably be provided due to the client's incapacity or an emergency situation, DOH may determine, using professional judgment, that the use or disclosure is in the client's best interests.

   1. Any agreement, objection, refusal, or restriction by the client, may be oral or in writing. DOH will document any such oral communication in the client's case file.

   2. DOH will also document in the case file the outcome of any opportunity provided to object; the client's decision not to object; or the inability of the client to object.

   NOTE: Verbal permission to use or disclose information for purposes described in this section is not sufficient when the client is referred

to or receiving substance abuse treatment. Written authorization is required under those circumstances.

Re-disclosure of a Client's Information:

A. Unless prohibited by state and federal laws, information held by DOH and authorized by the client for disclosure to a third party may be subject to re-disclosure by the third party. In such cases, the information is no longer protected by DOH or covered by its policy.

B. Alcohol and drug rehabilitation information: Federal regulations (42 CFR part 2 and 34 CFR 361.38) prohibit DOH from making further disclosure of alcohol and drug rehabilitation information without the specific written authorization of the client to whom it pertains.

Revocation of Authorization

A. A client can revoke an authorization at any time.

B. Any revocation must be in writing and signed by the client and maintained in the file.

Exception: Alcohol and drug treatment clients may orally revoke authorization to disclose information obtained from alcohol and drug treatment programs. Oral authorizations must be documented and maintained in the client's record.

C. No such revocation shall apply to information already released while the authorization was valid and in effect.

Verification of Client Requesting Information

PHI about a client may not be disclosed without verifying the identity of the person requesting the information in accordance with the appropriate Bureau or office policy and procedure, if the DOH staff member fulfilling the request does not know that person.

Denial of Requests for Information

Unless a client has signed an authorization, or the information about the client can be disclosed pursuant to this policy, DOH shall deny any request for client information.

Prohibition of Use or Disclosure of Client's PHI

DOH shall not use or disclose any client's PHI for marketing purposes, except where communication describes a prescription drug or biologic and DOH cannot receive compensation for the communication. Also DOH shall not use or disclose any client's PHI for any fund-raising activities.

Reference(s):

- 45 CFR 164.502(a)
- 45 CFR 164.508 – 164.512
- 42 CFR Part 2

Contact(s): •

Privacy Program Office, (615-741-1969)

Tennessee Department of Health

HIPAA Policies

Privacy

Policy Title: Minimum Necessary Information

Policy Number: 104

Effective Date: April 14, 2003 **Revised: February 18, 2010**

PURPOSE:

This policy limits the amount of PHI that is used or disclosed by DOH workforce members to the minimum necessary and to ensure that DOH employees have access to the information they require to accomplish DOH mission, goals and objectives.

POLICY:

General

A. DOH will use or disclose only the minimum amount of PHI necessary to provide services and benefits to clients, and only to the extent provided in DOH policies and procedures.

B. This policy does not apply to:

1. Disclosures to or requests by a health care provider for treatment;

2. Disclosures made to the client about his or her own protected information;

3. Uses or disclosures authorized by the client that are within the scope of the authorization;

4. Disclosures made to the United States Department of Health and Human Services, Office for Civil Rights, in accordance with subpart C of part 160 of the HIPAA Privacy Rule;

5. Uses or disclosures that are required by law; and

6. Uses or disclosures required for compliance with the HIPAA transaction rule. The minimum necessary standard does not apply to the required or situational data elements specified in the implementation guides under the transaction rule.

Minimum Necessary Information

NOTE: Until guidance is published, by Secretary of HHS on what constitutes "minimum necessary" for use or disclosures of PHI, DOH must to the extent practicable, limit use, disclosure or request of PHI to the "limited data set" (Defined as PHI without names, address, telephone/fax, email, SSN, MRN and 9 other identifiers (As outlined in DOH HIPAA Policy # 107 *De-identification of Client Information and Use of Limited data Sets* under Requirements for De-identification of Client Information Section B.), or if needed the minimum necessary to accomplished the intended purpose.

A. When DOH policy permits use or disclosure of a client's PHI to another entity, or when DOH requests a client's PHI from another entity, DOH employees must make reasonable efforts to limit the amount of information to the minimum necessary needed to accomplish the intended purpose of the use, disclosure, or request.

B. If DOH policy permits making a particular disclosure to another entity, DOH employees may rely on a requested disclosure as being the minimum necessary for the stated purpose when:

1. Making disclosures to public officials that are permitted under 45 CFR 164.512, and as stated in **DOH HIPAA Policy #103,** "Uses and Disclosures of Client or Participant Information," if the public official states that the information requested is the minimum necessary for the stated purpose(s). A "public official" is any

employee of a government agency who is authorized to act on behalf of that agency in performing the lawful duties and responsibilities of that agency.

2. The information is requested by another entity that is a "covered entity" under the HIPAA privacy rules. A "covered entity" is a health plan, a health care provider who conducts electronic transactions, or a health care clearinghouse;

3. The information is requested by a professional who is a member of the workforce of DOH or is a business associate of DOH for the purpose of providing professional services to DOH, if the professional represent that the information requested is the minimum necessary for the stated purpose(s); or

4. Documentation or representations that comply with the applicable requirements of **DOH HIPAA Policy #106**, "Use and Disclosure for Research Purposes & Waivers" have been provided by a person requesting the information for research purposes.

Access & Uses of Information

A. DOH will make reasonable efforts to limit each workforce member's access to only the PHI that is needed to carry out his/her duties. These efforts will include internal staff to staff use and disclosure of PHI.

B. Each bureau/office will determine, by category of responsibilities or by individual responsibilities, what level of PHI the workforce members will have access to in order to carry out their duties. Once the determinations have been made, the employees will be informed. The determinations will be documented and shall include their accessibility to electronic, as well as, paper format for PHI.

Routine and Recurring Disclosure of a Client's Information

A. For routine and recurring disclosures (including disclosure in routine reports), DOH program areas will:

1. Determine who is requesting the information and the purpose for the request. If the request is **not** compatible with the purpose for which it was collected, refer to and apply the "non-routine use" procedures in the following section.

2. Confirm that the applicable DOH policies permit the requested use (disclosure is consistent with the program purposes), and that the nature or type of the use recurs (occurs on a periodic basis) within the program or activity;

3. Identify the kind and amount of information that is necessary to respond to the request; and

4. If the disclosure is one that must be included in the DOH accounting of disclosures, include required documentation required by the appropriate bureau or office.

B. For the purposes of this policy, "routine and recurring" means the disclosure of records outside DOH, without the authorization of the client, for a purpose that is compatible with the reason for which the information was collected. The following identifies several examples of uses and disclosures that DOH has determined to be compatible with the purposes for which information is collected.

1. DOH will not disclose a client's entire medical record unless the request specifically justifies why the entire medical record is needed.

2. Routine and recurring uses include disclosures required by law. For example, a mandatory child abuse report by a DOH employee would be a routine use.

3. When federal or state agencies – such as the DHHS Office for Civil Rights, the DHHS Office of Inspector General, the State of Tennessee Medicaid Fraud Unit, or the Tennessee Comptroller Office – have the legal authority to require DOH to produce records necessary to carry out audit or oversight of DOH programs or activities, DOH will make such records available as a routine and recurring use.

4. When the appropriate DOH official determines that records are subject to disclosure under Tennessee law, DOH may make the disclosure as a routine and recurring use.

Non-routine Disclosure of a Client's Information

A. For the purpose of this policy, "non-routine disclosure" means the disclosure of records outside DOH (whether in an ad hoc report or record) that is not for a purpose for which it was collected.

B. DOH will not disclose a client's entire medical record unless the request specifically justifies why the entire medical record is needed, and applicable laws and policies permit the disclosure of all the information in the medical record to the requestor.

C. Requests for non-routine disclosures must be reviewed on an individual basis to limit the information disclosed to only the minimum amount of information necessary to accomplish the purpose for which the disclosure is sought.

DOH Request for a Client's PHI from Another Entity

When requesting information about a client from another entity, DOH employees must limit requests to those that are reasonably necessary to accomplish the purpose for which the request is made. DOH will not request a client's entire medical record unless DOH can specifically justify why the entire medical record is needed.

Reference(s):
• 45 CFR Parts 160 and 164

Contact(s):
• Privacy Program Office, 615-741-1969

Tennessee Department of Health

HIPAA Policies

Privacy

Policy Title: Administrative, Technical, and Physical Safeguards

Policy Number: 105

Effective Date: April 14, 2003

PURPOSE:

The intent of this policy is to establish criteria for safeguarding protected health information (PHI) and to minimize the risk of unauthorized access, use or disclosure.

POLICY:

General

DOH must take reasonable steps to safeguard information from any intentional or unintentional use or disclosure that is in violation of the privacy policies.

Information to be safeguarded may be in any medium, including paper, electronic, verbal, and visual representations of PHI.

Safeguarding PHI Information – DOH Workplace Practices

A. Paper

1. DOH staff must make reasonable efforts to ensure the safeguarding of PHI including the use of locked storage wherever available, and ensuring the safeguarding of PHI.

2. Each DOH workplace will ensure that the disposal of files and documents is performed on a timely basis, consistent with record retention requirements and are subject to the same safeguarding requirements until destruction occurs.

B. Verbal:

1. DOH staff must take reasonable steps to protect the privacy of all verbal exchanges or discussions of PHI, regardless of where the discussion occurs.

2. Each DOH workplace must ensure employee awareness of the potential for inadvertent verbal disclosure of PHI.

C. Visual:

1. Each DOH workplace must make every effort to ensure that PHI is not visible to unauthorized persons. This would include PHI on desk tops, computer screens, fax machines, photocopy machines, printers, management reports or other paper documents in accordance with the appropriate bureau or office policy and procedure.

Safeguarding PHI – DOH Administrative Safeguards

A. A determination of who should have access to the specific data will be established in each bureau and office and program area.

1. DOH managers and supervisors will determine the role of each of their staff members and request exceptions based on the needs of their office.

2. Managers are responsible for allowing access to enough information for their staff to do their jobs while holding to the minimum necessary standard.

B. DOH managers and supervisors will:

1. Safeguard confidential information;

2. Conduct a thorough assessment of each category of responsibilities and/or individual employee;

3. Foster a more secure atmosphere and enhance the belief that confidential information is important and that protecting privacy is key to achieving DOH goals.

4. Managers will update the safeguards in place each year, seeking to achieve reasonable administrative, technical and physical safeguards.

C. Utilize the security policies when they are developed to augment safeguard procedures.

D. DOH staff will be required to sign a "confidentiality statement" that constitutes a formal commitment to adhere to the department-wide privacy and security policies concerning the PHI.

Contact(s):

• Privacy Program Office, (615) 253-5417

Tennessee Department of Health

HIPAA Policies

Privacy

Policy Title: Use and Disclosure for Research Purposes and Waivers

Policy Number: 106

Effective Date: April 14, 2003

PURPOSE:

The intent of this policy is to specify when DOH may use or disclose information about clients for research purposes.

POLICY:

General

When DOH uses or discloses a client's protected health information (PHI) for research purposes, they must consider the following:

A. DOH may use or disclose a client's information for research purposes as specified in this policy. "Research" means "a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalized knowledge."

B. All such research disclosures are subject to applicable requirements of state and federal laws and regulations and to the specific requirements of this policy.

NOTE: This policy is intended to supplement existing research requirements of the Common Rule, 45 CFR Part 46. The Common Rule is the rule for the protection of human subjects in research promulgated by the U.S. Department of Health and Human

Services, and adopted by other federal governmental agencies, including the National Institutes for Health, for research funded by those agencies. In addition, some agencies have requirements that supplement the Common Rule that are applicable to a particular research contract or grant.

C. De-identified information may be used or disclosed for purposes of research, consistent with **DOH HIPAA Policy #107**, *"De-identification of Client Information and Use of Limited Data Sets."*

D. A limited data set may be used or disclosed for purposes of research, consistent with the policies related to limited data sets in **DOH HIPAA Policy #107**, *"De-identification of Client Information and Use of Limited Data Sets."*

E. DOH may also conduct public health studies, studies that are required by law, and studies or analysis related to its health care operations. Such studies will be discussed in sections of this policy.

Institutional Review Board (IRB) or Privacy Board Established by DOH

DOH may use an IRB established in accordance with 45 CFR Part 46 or a privacy board that has been established by DOH pursuant to this policy, to perform the duties and functions specified in this policy regarding a research project being conducted, in whole or in part, by DOH or by a DOH office or program.

Uses and Disclosures for Research Purposes – Specific Requirements

A. DOH may use or disclose client information for research purposes with the client's specific written authorization.

1. Such authorization must meet all the requirements described in **DOH HIPAA Policy #103**, *"Uses and Disclosures of Client Information,"* and may indicate as an expiration date such terms as "end of research study," or similar language.

2. An authorization for use and disclosure for a research study may be combined with any other type of written permission for the same research study.

3. If research includes treatment, the researcher may condition the provision of research related treatment on the provision of an authorization for use and disclosure for such research.

B. DOH may use or disclose client PHI for research purposes without the client's written authorization provided that:

1. DOH obtains documentation that a waiver of a client's authorization for release of information requirements has been approved by either:

   a. An institutional review board (IRB); or

   b. A privacy board that:

      i) Has members with varying backgrounds and appropriate professional competency as needed to review the effect of the research protocol on the client's privacy rights and related concerns;

      ii) Includes at least one member who is not affiliated with DOH, not affiliated with any entity conducting or sponsoring the research, and not related to any person who is affiliated with any such entity; and

      iii) Does not have any member participating in a review of any project in which the member has a conflict of interest.

2. Documentation required of IRB or privacy board when granting approval of a waiver of an client's authorization for release of PHI must include:

   a. A statement identifying the IRB or privacy board that approved the waiver of an client's authorization, and the date of such approval;

   b. A statement that the IRB or privacy board has determined that the waiver of authorization, in whole or in part, satisfies the following criteria:

i) The use or disclosure of an client's PHI involves no more than minimal risk to the privacy of clients, based on at least the following elements:

- An adequate plan to protect a client's identifying PHI from improper use or disclosure;

- An adequate plan to destroy a client's identifying PHI at the earliest opportunity consistent with the conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and

- Adequate written assurances that the PHI will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure of the PHI would be permitted under this policy;

The research could not practicably be conducted without the waiver; and

- The research could not practicably be conducted without access to and use of the client's PHI;

- A brief description of the PHI for which use or disclosure has been determined to be necessary by the IRB or privacy board;

- A statement that the waiver of an client's authorization has been reviewed and approved under either normal or expedited review procedures, by either an IRB or a privacy board, pursuant to federal regulations at 45 CFR 164.512(2); and

- The privacy board chair must sign documentation of the waiver of a client's authorization, or other member as designated by the chair of the IRB or the privacy board, as applicable.

3. In some cases, a researcher may request access to client PHI maintained by DOH in preparation for research or to facilitate the development of a

research protocol in anticipation of research. Before agreeing to provide such access to client PHI, DOH should determine whether federal or state law otherwise permits such use or disclosure without client authorization or use of an IRB. If there is any doubt whether the use and disclosure of the information by the researcher falls within this HIPAA exception, review by an IRB or privacy board and formal waiver of authorization is required. If such access falls within this HIPAA exception to authorization and is otherwise permitted by other federal or state law, DOH will only provide such access if DOH obtains, from the researcher, written representations that:

a. Use or disclosure is sought solely to review a client's PHI needed to prepare a research protocol or for similar purposes to prepare for the research project;

b. No client PHI will be removed from DOH by the researcher in the course of the review; the client PHI for which use or access is sought is necessary for the research purposes;

c. Researcher and his or her agents agree not to use or further disclose the information other than as provided in the written agreement, and to use appropriate safeguards to prevent the use or disclosure of the information other than is provided for by the written agreement;

d. Researcher and his or her agents agree not to publicly identify the information or contact the client whose data is being disclosed; and

e. Applicable federal or state law may require such other terms or conditions.

4. In some cases, a researcher may request access to PHI maintained by DOH about clients who are deceased. DOH should determine whether federal or state law otherwise permits such use or disclosure of information about decedents without client authorization or use of an IRB. There may be instances where it would be inappropriate to disclose information, even where the client subject of the information is dead – for example, clients who died of AIDS may not have wanted such information to be disclosed after their deaths. If there is any doubt, whether the use and disclosure of the information by the researcher falls within this HIPAA exception, review by an IRB or privacy board and formal waiver of authorization is required. If such access falls within

this HIPAA exception to authorization and is otherwise permitted by other federal or state law, DOH will only provide such access if DOH obtains the following written representations from the researcher:

a. Representation that the use or disclosure is sought solely for research on the PHI of deceased persons;

b. Documentation, if DOH so requests, of the death of such persons; and

c. Representation that the client's PHI for which use or disclosure is sought is necessary for the research purposes.

d. Researcher and his or her agents agree not to use or further disclose the information other than as provided in the written agreement, and to use appropriate safeguards to prevent the use or disclosure of the information other than is provided for by the written agreement;

e. Researcher and his or her agents agree not to publicly identify the information or contact the personal representative or family members of the decedent; and

f. Applicable federal or state law may require such other terms or conditions.

DOH Public Health Studies and Studies Required by Law

When DOH is operating as a public health authority, DOH is authorized to obtain and use client PHI without authorization for the purpose of preventing injury or controlling disease and for the conduct of public health surveillance, investigations and interventions. In addition to these responsibilities, DOH may collect, use or disclose information without client authorization, to the extent that such collection, use or disclosure is required by law. When DOH uses information to conduct studies pursuant to such authority, no additional client authorization is required nor does this policy require IRB or privacy board waiver of authorization based on the HIPAA privacy rules. Other applicable laws and protocols continue to apply to such studies.

DOH Studies Related to Health Care Operations

Studies and data analyses conducted for DOH'S own quality assurance purposes and to comply with reporting requirements applicable to federal or state funding requirements fall within the uses and disclosures that may be made without client authorization as DOH health care operations. Neither client authorization nor IRB or privacy board waiver of authorization is required for studies or data analyses conducted by of on behalf of DOH for purposes of health care operations, including any studies or analyses conducted to comply with reporting requirements applicable to federal or state funding requirements. "Health care operations" as defined in 45 CFR 164.512 includes:

A. Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that obtaining generalized knowledge is not the primary purpose of any studies resulting from such activities;

B. Conducting population-based activities relating to improving health care or reducing health care costs, protocol development, case management and care coordination, contacting health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;

C. Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, and conducting training programs, and accreditation, certification, licensing or credentialing activities;

D. Underwriting, premium rating, and other activities related to the creation, renewal or replacement of a contract of health insurance or health benefits;

E. Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;

F. Business planning and development, such as conducting cost-management and planning related analyses associated with managing and operating DOH, including improvement of administration or development or improvement of methods of payment or coverage policies; and

G. Business management and general administrative activities of DOH, including management activities related to HIPAA implementation and

compliance; customer services, including the provision of data analyses for other customers; resolution of internal grievances; and

H. Creating de-identified information or a limited data set consistent with the **DOH HIPAA Policy #107**, *"De-identification of Client Information and Use of Limited Data Sets."*

- **Exception:** HIV-AIDS information may not be disclosed to anyone without the specific written authorization of the client. Re-disclosure of HIV test information is prohibited, except in compliance with law or with written permission from the client.

Reference(s):

- 45 CFR Part 64
- 45 CFR 164.512

Contact(s):

- Privacy Program Office, (615) 253-5417

Tennessee Department of Health

HIPAA Policies

Privacy

Policy Title: De-identification of Client Information and Use of Limited Data Sets

Policy Number: 107

Effective Date: April 14, 2003

PURPOSE:

The intent of this policy is to prescribe standards under which client protected health information (PHI) can be used and disclosed without authorization or tracking of disclosures when all information that could identify a person has been removed or restricted to a limited data set. This policy does not apply to PHI transmitted to a business associate.

POLICY:

General

A. De-identified information is client information from which DOH or another entity has deleted, redacted, or blocked identifiers, so that the remaining information cannot reasonably be used to identify a person.

B. Unless otherwise restricted or prohibited by other federal or state law, DOH can use and share information as appropriate for the work of DOH, without further restriction, if DOH or another entity has taken steps to de-identify the information consistent with the requirements and restrictions defined in this policy.

C. DOH may use or disclose a limited data set that meets the requirements for a limited data set as defined in this policy, if DOH enters into a data use

agreement with the limited data set recipient (or with the data source, if DOH will be the recipient of the limited data set) in accordance with the requirements of a data use agreement as defined in this policy.

D. DOH may disclose a limited data set only for the purposes of research, public health or health care operation. However, unless DOH has obtained a limited data set that is subject to a data use agreement, DOH is not restricted to using a limited data set for its own activities or operations.

E. If DOH knows of a pattern or activity or practice of the limited data set recipient that constitutes a material breach or violation of a data set agreement, DOH will take reasonable steps to cure the breach or end the violation and, if such steps are unsuccessful, DOH will discontinue disclosure of information to the recipient and report the problem to the United States Department of Health and Human Services, Office for Civil Rights.

Requirements for De-identification of Client Information

DOH may determine that client information is sufficiently de-identified, and cannot be used to identify an individual, only if ***either*** 1 or 2 below have occurred:

A. A statistician or other person with appropriate knowledge of, and experience with, generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:

1. Has applied such principles and methods, and determined that the risk is minimal that the information could be used alone or in combination with other reasonably available information, by a recipient of the information to identify the person whose information is being used; and

2. Has documented the methods and results of the analysis that justify such a determination; ***or***

B. DOH has ensured that:

1. The following identifiers of the individual or of relatives, employers, and household members of the individual are removed:

   a. Names;

   b. All geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code, and their equivalent geo codes. However, the initial three digits of a zip code may remain on the information if, according to current publicly-available data from the Bureau of the Census, the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and the initial three digits for all such geographic units containing 20,000 or fewer people is changed to 000;

   c. All elements of dates (except year) for dates directly relating to an individual, including birth date, dates of admission and discharge from a health care facility, and date of death. For persons age 90 and older, all elements of dates (including year) that would indicate such age must be removed, except that such ages and elements may be aggregated into a single category of "age 90 or older;"

   d. Telephone numbers;

   e. Fax numbers;

   f. Electronic mail addresses;

   g. Social security numbers;

   h. Medical record numbers;

   i. Health plan beneficiary numbers;

   j. Account numbers;

   k. Certificate or license numbers;

l. Vehicle identifiers and serial numbers, including license plate numbers;

m. Device identifiers and serial numbers;

n. Web Universal Resource Locators (URLs);

o. Internet Protocol (IP) address numbers;

p. Biometric identifiers, including fingerprints and voiceprints;

q. Full face photographic images and any comparable images; and

r. Any other unique identifying number, characteristic, or codes, except as permitted under the Re-identification section below, of this policy; ***and***

2. DOH has no actual knowledge that the information could be used alone or in combination with other information to identify an individual who is the subject of the information.

C. The DOH Privacy Officer will designate the statistician or other person referred above, who may be either:

1. A DOH employee;

2. An employee of another governmental agency; or

3. An outside contractor or consultant, subject to DOH contract and personnel policy.

Re-identification of De-identified Information

DOH may assign a code or other means of record identification to allow information de-identified under this policy to be re-identified by DOH, except that:

1. The code or other means of record identification is not derived from or related to information about the individual and cannot otherwise be translated to identify the individual; and

2. DOH does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification.

Requirements for a Limited Data Set

A limited data set is information that excludes the following direct identifiers of the individual, or of relatives, employers or household members of the individual:

1. Names;

2. Postal address information, other than town or city, state and zip code;

3. Telephone numbers;

4. Fax numbers;

5. Electronic mail addresses;

6. Social Security numbers;

7. Medical record numbers;

8. Health plan beneficiary numbers (such as Medicaid Prime Numbers);

9. Account numbers;

10. Certificate/license numbers;

11. Vehicle identifiers and serial numbers, including license plate numbers;

12. Web Universal Resource Locators (URLs);

13. Internet Protocol (IP) address numbers;

14. Biometric identifiers, including finger and voice prints; and

15. Full face photographic images and any comparable images.

Contents of a Data Use Agreement

A. DOH may disclose a limited data set only if the entity receiving the limited data set enters into a written agreement with DOH, in accordance with subsection (B) immediately below, that such entity will use or disclose the protected health information only as specified in the written agreement.

B. A data use agreement between DOH and the recipient of the limited data set must:

1. Specify the permitted uses and disclosures of such information by the limited data set recipient. DOH may not use the agreement to authorize the limited data set recipient to use or further disclose the information in a manner that would violate the requirements of this policy if done by DOH.

2. Specify who is permitted to use or receive the limited data set; and

3. Specify that the limited data set recipient will:

   a. Not use or further disclose the information other than as specified in the data use agreement or as otherwise required by law;

   b. Use appropriate safeguards to prevent use or disclosure of the information other than as specified in the data use agreement;

   c. Report to DOH if the recipient becomes aware of any use or disclosure of the information not specified in its data use agreement with DOH;

   d. Ensure that any agents to whom it provides the limited data set (including a subcontractor), agrees to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and

e. Not identify the information or contact the individuals whose data is being disclosed.

Reference(s):
• 45 CFR 164.514
Contact(s):
• Privacy Program Office, (615) 253-5417

Tennessee Department of Health

HIPAA Policies

Privacy

Policy Title: Business Associates

Policy Number: 108

Effective Date: April 14, 2003

PURPOSE:

The purpose of this policy is to specify when DOH may disclose a client's protected health information (PHI) to a business associate of DOH, and to specify provisions that must be included in DOH contracts with business associates.

POLICY:

General

A. DOH has many contractual and business relationships, and DOH has a policy related to its contracts and business relationships. However, not all contractors or business partners are "business associates" of DOH. This policy only applies to contractors or business partners that come within the definition of a "business associate."

B. If a contractor or business partner is a "business associate," those contracts that define the contractual relationship remain subject to all federal and state laws and policies governing the contractual relationship. A "business associate" relationship also requires additional contract provisions. The additional contract requirements are described in this policy.

C. "Business Associate" means (per 45 CFR 160.103):

1. With respect to DOH, a person or entity who:

   a. On behalf of DOH, but other than in the capacity of a DOH workforce member, performs or assists in the performance of a function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, utilization review, quality assurance, billing benefit management, or

   b. Provides, other than in the capacity of a DOH employee, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for DOH, where the provision of the service involves the disclosure of individually identifiable health information from DOH, or from another business associate of DOH, to the person.

2. A covered entity may be a business associate of another covered entity.

D. A business associate relationship is formed only if protected health information is to be used, created, or disclosed in the relationship.

E. The following are not business associates or business associate relationships:

1. DOH workforce members;

2. Medical providers providing treatment to clients;

3. Enrollment or eligibility determinations, involving DOH clients, between government agencies;

4. Payment relationships, such as when DOH is paying medical providers, or other entities for services to DOH clients when the entity is providing its own normal services that are not on behalf of DOH;

5. When a client's protected health information is disclosed based solely on a client's authorization;

6. When a client's protected health information is not being disclosed by DOH or created for DOH; and

7. When the only information being disclosed is information that is de-identified in accordance with **DOH HIPAA Policy #107**, *"De-identification of Client or Participant Information and Use of Limited Data Sets."*

8. Persons or organizations (e.g.) janitorial services) whose duties do not involve the use or disclosure of PHI and where any access to PHI by such persons would be incidental, if at all.

F. DOH may disclose a client's protected health information to a business associate and may allow a business associate to create or receive a client's protected health information on behalf of DOH, if:

1. DOH first enters into a written contract, or other written agreement or arrangement, with the business associate before disclosing a client's protected health information to the business associate, in accordance with the contract requirements specified in this policy.

2. The written contract or agreement provides satisfactory assurance that the business associate will appropriately safeguard the information.

Contract Requirements Applicable to Business Associates

A. A contract between DOH and a business associate must include terms and conditions that:

1. Establish the permitted and required uses and disclosures of protected health information by the business associate. The contract may not authorize the business associate to further use or disclose health information obtained from DOH, except that the contract may permit the business associate to:

a. Use and disclose protected health information for the proper management and administration of the business associate; and

b. Collect data relating to DOH operations.

2. Provide that the business associate will:

   a. Not use or further disclose protected health information other than as permitted or required by the contract or as required by law;

   b. Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the contract;

   c. Report to DOH any use or disclosure not allowed by the contract of which the business associate becomes aware;

   d. Ensure that any agents or subcontractors to whom it provides protected health information agrees to the same restrictions and conditions that apply to the business associate under the contract;

   e. Ensure that business associates have mechanisms in place to protect clients' rights regarding PHI;

   f. Make its internal practices, books, and records relating to the use and disclosure of protected health information available to DOH and to the United States DHHS for the purpose of determining DOH compliance with federal requirements; and

   g. At termination of the contract, if reasonably feasible, return or destroy all protected health information that the business associate still maintains in any form, and keep no copies thereof. If not feasible, the business associate will continue to protect the information.

3. Authorize termination of the contract if DOH determines that the business associate has violated a material term of the contract.

B. If the business associate of DOH is another governmental entity:

1. DOH may enter into a memorandum of understanding, rather than a contract, with the business associate if the memorandum of understanding contains terms covering all objectives of the contract requirements outlined in this policy;

2. The written contract, agreement, or memorandum does not need to contain specific provisions required under 2.a., above, if other law or regulations contain requirements applicable to the business associate that accomplish the same objective;

C. If a business associate is required by law to perform a function or activity on behalf of DOH or to provide a service to DOH, DOH may disclose protected health information to the business associate to the extent necessary to enable compliance with the legal requirement without a written contract or agreement, if:

1. DOH attempts in good faith to obtain satisfactory assurances from the business associate that the business associate will protect health information to the extent specified in 2.a., above; and

2. If such attempt fails, DOH documents the attempt and the reasons that such assurances cannot be obtained;

D. Other requirements for written contracts or agreements:

The written contract or agreement between DOH and the business associate may permit the business associate to:

1. Use information it receives in its capacity as a business associate to DOH, if necessary:

   a. For proper management and administration of the business associate; or

   b. To carry out its legal responsibilities.

2. Disclose information it receives in its capacity as a business associate if:

   a. The disclosure is required by law; or

b. The business associate receives assurances from the person to whom the information is disclosed that:

i) It will be held or disclosed further only as required by law or for the purposes to which it was disclosed to such person; and

ii) The person notifies the business associate of any known instances in which the confidentiality of the information has been breached.

Responsibilities of DOH in Business Associate Relationships

A. DOH responsibilities in business associate relationships include, but are not limited to, the following:

1. Receiving and logging a client's complaints regarding the uses and disclosures of protected health information by the business associate or the business associate relationship;

2. Receiving and logging reports from the business associate of possible violations of the business associate contracts;

3. Implementation of corrective action plans, as needed; and

4. Mitigation, if necessary, of any known violations up to and including contract termination.

B. DOH will provide business associates with applicable contract requirements, and may provide consultation to business associates as needed on how to comply with contract requirements regarding protected health information.

Business Associate Non-compliance

A. If DOH knows of a pattern of activity or practice of a business associate that constitutes a material breach or violation of the business associate's obligation under the contract or other arrangement, DOH must take reasonable steps to cure the breach or end the violation, as applicable, including working with and providing consultation to the business associate.

B. If such steps are unsuccessful, DOH must:

1. Terminate the contract or arrangement, if feasible; or

2. If termination is not feasible, report the problem to the United States DHHS.

Reference(s):

- 45 CFR 160 & 164

Contact(s):

- Privacy Program Office, (615) 253-5417

Tennessee Department of Health

HIPAA Policies

Privacy

Policy Title: Enforcement, Sanctions, and Penalties for Violations of Individual Privacy

Policy Number: 109

Effective Date: April 14, 2003

PURPOSE:

The intent of this policy is to specify enforcement, sanction, penalty, and disciplinary actions that may result from violation of DOH policies regarding the privacy and protection of an individual's information and to offer guidelines on how to conform to the required standards.

POLICY:

General

A. All employees, volunteers, interns and members of the DOH workforce must guard against improper uses or disclosures of a DOH client or provider's information.

   1. DOH employees, volunteers, interns and members of the DOH workforce who are uncertain if a disclosure is permitted are advised to consult with a supervisor in the DOH workplace. The Department Privacy Officer may be consulted on any disclosure question.

B. All employees are required to be aware of their responsibilities under DOH privacy policies and will be expected to sign a "Confidentiality Statement" (Form-3131) indicating that they have been informed of the business practices in DOH as it relates to privacy, and they understand their

responsibilities to ensure the privacy of DOH clients and participants.

C. Supervisors are responsible for assuring that employees who have access to PHI, whether it be electronic, hard copy, or verbally, are informed of their responsibilities.

D. DOH employees who violate DOH policies and procedures regarding the safeguarding of an individual's information are subject to appropriate disciplinary action by DOH up to and including immediate dismissal from employment, and/or legal action by the individual, who may want to pursue a tort claim against the State of Tennessee or a lawsuit against the state and the employee.

E. DOH employees who knowingly and willfully violate state or federal law for improper use or disclosure of an individual's information are subject to criminal investigation and prosecution or civil monetary penalties and may be enforced by the federal Department of Health and Human Services.

F. If DOH, as a state agency, **fails to enforce privacy safeguards DOH may be subject to administrative penalties by the Department of Health and Human Services (DHHS), including federal funding penalties.**

Retaliation Prohibited

Neither DOH as an entity, nor any DOH employee will intimidate, threaten, coerce, discriminate against, or take any other form of retaliatory action against:

1. Any individual for exercising any right established under DOH policy, or for participating in any process established under DOH policy, including filing a complaint with DOH or with DHHS.

2. Any individual or other person for:

   a. Filing a complaint with DOH or with DHHS as provided in DOH privacy policies;

   b. Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing relating to DOH policy and procedures; or

   c. Opposing any unlawful act or practice, provided that:

i. The individual or other person (including a DOH employee) has a good faith belief that the act or practice being opposed is unlawful; and

ii. The manner of such opposition is reasonable and does not involve a use or disclosure of an individual's protected information in violation of DOH policy.

Disclosures by Whistleblowers and Workforce Crime Victims

A. A DOH employee may disclose limited PHI about an individual to a law enforcement official if the employee is the victim of a criminal act and the disclosure is:

1. About only the suspected perpetrator of the criminal act; and

2. Limited to the following information about the suspected perpetrator:

a. Name and address;

b. Date and place of birth;

c. Social security number;

d. ABO blood type and Rh factor;

e. Type of any injury;

f. Date and time of any treatment; and

g. If applicable, date and time of death;

B. A DOH employee or business associate may disclose an individual's protected client information if:

1. The DOH employee or business associate believes, in good faith, that DOH has engaged in conduct that is unlawful or that otherwise violates professional standards or DOH policy, or that the care, services, or conditions provided by DOH could endanger DOH staff, persons in

DOH care, or the public; and

2. The disclosure is to:

   a. An oversight agency or public authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of DOH;

   b. An appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or of misconduct by DOH; or

   c. An attorney retained by or on behalf of the DOH employee or business associate for the purpose of determining the legal options of the DOH employee or business associate with regard to this DOH policy.

Reference(s):

- 45 CFR 164.530

Contact(s):

- Privacy Program Office, (615) 253-5417

Tennessee Department of Health

HIPAA Policies

Privacy

Policy Title: Mitigation Efforts

Policy Number: 110

Effective Date: April 14, 2003

PURPOSE:

The purpose of this policy is to specify the extent that mitigation must take place.

General

DOH has the duty to mitigate "to the extent practicable," any harmful effects due to uses or disclosures of protected health information (PHI) in violation of the regulations or DOH policies.

The duty to mitigate arises only when DOH has actual knowledge of inappropriate use or disclosure of PHI either by DOH or a business associate. Bureaus/offices are required to take "reasonable steps" to reduce harmful effects of those actions about which they are aware.

Bureaus/offices are obligated to undertake reasonable close monitoring of the activities of members of their workforce. When unauthorized uses or disclosures of PHI take place, precautions should be put in place to ensure that similar disclosures do not occur in the future. If the disclosure is made by DOH workforce, appropriate action should take place immediately.

The Department Privacy Officer shall be notified immediately when unauthorized uses or disclosures take place either internally or externally to determine if mitigation efforts should be undertaken.

Tennessee Department of Health

HIPAA Policies

Privacy/Security

Policy Title: **Breach Notification of Unsecured Protected Health Information**

Policy Number: 111

Effective Date: February 18, 2010

PURPOSE:

The intent of this policy is to establish criteria for issuing a notification in the case of a breach of unsecured Protected Health Information (PHI).

POLICY:

General

DOH must notify clients promptly if their unsecured PHI has been or is reasonably believed to have been breached. A breach is defined as "the acquisition, access, use, or disclosure" of PHI in a manner that violates the HIPAA Rules and also "compromises the security or privacy of the PHI."

"Unsecured" PHI is PHI that is "not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by HHS."

A breach that "compromises the security or privacy of the PHI" is that which "poses a **significant risk of financial, reputational, or other harm** to the individual." The risk of harm standard requires DOH to determine in good faith whether it is necessary to notify the individual of the breach. The following factors should be considered in determining the risk of harm:

1. **Nature of the Data Elements Breached.** DOH should analyze the nature of the data elements compromised. For example, the disclosure of a person's name in one context may be more sensitive than the disclosure of a name in another context.
2. **Likelihood the Information is Accessible and Usable.** DOH should assess the likelihood that unsecured PHI will be, or has been, used by unauthorized individuals.
3. **Likelihood the Breach May Lead to Harm.** In the context of the type(s) of data involved in the breach, DOH should consider the number of possible harms that could arise as a result of the breach of unsecured PHI, and further assess the likelihood of harm.
4. **Ability of DOH to Mitigate the Risk of Harm.** The risk of harm may depend upon the ability of DOH to mitigate the effects of the breach. DOH should consider appropriate breach prevention, monitoring, and mitigation that it can take in response to the breach.

Breach Exceptions

Exceptions to the definition of a breach are:

1. any unintentional access or use of PHI by a workforce member of DOH or person acting under DOH authority, if such access was in good faith, within that person's scope of authority, and did not result in further impermissible use or disclosure of the PHI;
2. any inadvertent disclosure by a person who is authorized to have access to such PHI to another authorized person in DOH or a Business Associate and the PHI is not further used or disclosed in an impermissible manner; and
3. a disclosure of PHI where DOH has good faith belief that the unauthorized person who received the PHI would not reasonably have been able to retain such PHI.

Notification to Privacy Officer

The staff/workforce members must immediately inform the DOH Privacy Officer upon becoming aware or informed of a breach. The DOH Privacy Officer upon learning of such will no later than seven (7) days commence investigation of the reported breach.

Breach Response Team

A DOH Breach Response Team will be established by DOH for the purpose of receiving and reviewing all breach notifications of unsecured PHI, so as to determine: (1) whether a breach of unsecured PHI has occurred, (2) analyze the nature of the data elements allegedly compromised, (3) the likelihood the information is accessible and usable, (4) the likelihood the breach may lead to harm, (5) and the ability of DOH to mitigate the risk of harm.

The Breach Response Team shall be made up of a representative from the DOH Office of Human Resources, the DOH Privacy Officer, the DOH Security Officer, the DOH Office for Information Technology Services, the DOH Office of General Counsel, the DOH Office of Internal Audit, and a representative from the DOH division or office in which the breach occurred.

Following completion of the investigation by the Privacy and Security Officers, the Privacy Officer will convene the Breach Response Team within a reasonable time but no later than thirty (30) days following the completion of the initial investigation, to review the results of the investigation so as to determine how the matter should be handled.

Notification to Individual

DOH must notify the affected individual(s) "without unreasonable delay" and in no case later than 60 calendar days after DOH became aware of the breach.

The notice shall be made in writing, except when DOH does not have the correct contact information for the individual or where there is particular urgency to the notification. The notice to the individual(s) must contain the following five (5) elements:

1. A brief description of what occurred with respect to the breach, including, to the extent known, the date of the breach and the date on which the breach was discovered;

2. A description of the types of unsecured PHI that were disclosed during the breach;
3. A description of the steps the individual should take in order to protect himself or herself from potential harm caused by the breach:
4. A description of what DOH is doing to investigate and mitigate the breach and to prevent future breaches; and
5. Instructions for the individual to contact the DOH.

The notice must be approved by the Breach Notification Team before it is sent to the affected individual.

Other Notice Requirements

If the breach of the unsecured PHI involves more than 500 clients of the department, DOH must notify media outlets within the state. The DOH must also notify the Secretary of HHS of any breach involving 500 or more people. Notification to the media and the Secretary must be made within 60 days of the discovery of the breach. The Privacy Officer will notify the Secretary. The notification to the media outlet will be handled through the DOH's Communications Office in conjunction with the Privacy Officer. The Privacy Officer shall provide a copy of the log of all breaches to the Secretary within 60 days after the end of the calendar year.

Training Employees

DOH Privacy Officer must ensure that all current and new employees, including management are trained on this new policy within a reasonable period of time after the policy becomes effective.

Reference(s):

- 45 CFR 160 & 164, Subpart D

Contact(s):

- Privacy Officer (615) 741-1969
- Security Officer (615) 741-0899